Allgemeine Richtlinie für Informationssicherheit und Datenschutz Sekundarschule Hausen am Albis, Kappel am Albis und Rifferswil

Änderungskontrolle

Version	Datum	Beschreibung, Bemerkung	Name
1.1	27.08.2025	Grundlagendokument erstellt	B. Moser & S. Zemp

Inhalt

1 Einleitung

Die Sekundarschule Hausen am Albis, Kappel am Albis und Rifferswil (Sek Hausen) ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme nach § 7 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verabschiedet die Schulpflege diese allgemeine Richtlinie. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Sek Hausen angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Richtlinie eine Beschreibung der Informationssicherheitsorganisation.

2 Allgemeine Bestimmungen

2.1 Gegenstand und Zweck

Diese Richtlinie regelt die Ziele, die Organisation der Sek Hausen und die allgemeinen Vorgaben in Bezug auf Datenschutz und Informationssicherheit sowie die Prozesse zu deren kontinuierlichen Verbesserung.

Sie ist angelehnt an die Allgemeine sowie die Besonderen Informationssicherheitsrichtlinien des Kantons Zürich.

Ausnahmen zu den in dieser Richtlinie definierten Vorgaben sind durch die Schulpflege bewilligen zu lassen.

2.2 Geltungsbereich

Die Allgemeine Richtlinie für Informationssicherheit und Datenschutz und die damit zusammenhängenden Dokumente (insbesondere die Weisung zur Informationssicherheit, das Rollen- und Berechtigungskonzept, die Massnahmen zur Sensibilisierung der Mitarbeitenden sowie das Notfallkonzept) gelten für alle Mitarbeiterinnen und Mitarbeiter der Sek Hausen.

Vertragspartner, die Daten bearbeiten, werden ebenfalls zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet. Zudem bildet die Technische Richtlinie für den Betrieb von Informationssystemen einen integrierenden Bestandteil für die detaillierte technische Umsetzung der in dieser Richtlinie formulierten Anforderungen.

2.3 Grundlagen

Die gesetzlichen Grundlagen für die Sek Hausen sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

3 Informationssicherheitsniveau

Die Massnahmen der Sek Hausen zur Sicherstellung von Datenschutz und Informationssicherheit sind auf einen normalen Schutzbedarf auszurichten. Diese Einstufung erfolgt aufgrund

- der Tatsache, dass die Sek Hausen Daten bearbeitet, die einen erhöhten Schutz vor unberechtigten Zugriffen und vor unerlaubten Änderungen benötigen (Personendaten und besondere Personendaten bzw. Persönlichkeitsprofile),
- der Anzahl Schülerinnen und Schüler: +/- 186
- der Unterstützung aller wesentlichen Funktionen und Aufgaben durch IKT- und Netzwerksysteme,
- der Tatsache, dass ein Ausfall von IKT- und Netzwerksystemen die Aufgabenerfüllung nicht beeinträchtigen darf.

4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 7 IDG):

Integrität	Informationen müssen richtig und vollständig sein.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verantwortung	Die politischen Behörden und die Mitarbeiterinnen und Mitarbeiter der Schule sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT[1]-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

5 Informationssicherheitsorganisation

5.1 Einleitung

Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert.

Die Schulpflege, die oder der Informationssicherheitsverantwortliche (ISV) und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es der Sek Hausen, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeiterinnen und Mitarbeiter sind die Voraussetzung dafür, dass die Sekundarschule Hausen am Albis die gesteckten Informationssicherheitsziele erreichen kann. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

Die Informationssicherheitsorganisation der Sek Hausen ist im Anhang A – Organigramm Sekundarschule Hausen am Albis definiert.

[1] Informations- und Kommunikationstechnologien (IKT) umfasst alle technischen Medien, die für die Handhabung von Informationen und zur Unterstützung der Kommunikation eingesetzt werden; hierzu zählen unter andere, Computer- und Netzwerkhardware sowie die zugehörige Software.

5.2 Schulpflege

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit in der Sek Hausen. Sie legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel. Sie weist die Rolle/Funktion Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher (ISV) und Datenschutzberaterin/Datenschutzberater einer verantwortlichen Person zu.

5.3 Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher

Für die Umsetzung der Informationssicherheitsziele, der Überwachung der Einhaltung des angestrebten Sicherheitsniveaus und für die Informationssicherheit ist die/der ISV verantwortlich ist. Sie/er ist für die Umsetzung der Sicherheitsrichtlinien und deren Kontrolle zuständig und berichtet in dieser Funktion direkt der Schulpflege Ressort Informatik und Kommunikation.

Der oder dem ISV werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer/seiner Tätigkeit zur Verfügung gestellt. Die Anwendungs- und Datenverantwortlichen sowie die IKT-Benutzerinnen und -Benutzer unterstützen sie/ihn in ihrer/seiner Tätigkeit. Sie/er wird in alle IKT-relevanten Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

Die/der ISV entscheidet über sicherheitsrelevante Fragen und verwaltet allfällige Ausnahmen. Sie/er ist die Anlaufstelle für Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Aufgaben der/des ISV:

- Betreuung der IKT-Umgebung der Sek Hausen und Schnittstelle zu externen Betreibern (in Zusammenarbeit mit der/dem TICTS)
- Initialisieren, überwachen und kontrollieren der Richtlinien zur Informationssicherheit
- Führen des IKT-Inventars (in Zusammenarbeit mit der/dem TICTS)
- Verwaltung von Domainnamen der Sek Hausen, insbesondere rechtzeitige Verlängerung der Registrierung (in Zusammenarbeit mit der/dem TICTS)
- Verwaltung der digitalen Zertifikate (wo vorhanden) inklusive Überwachung der Gültigkeitsdauer (in Zusammenarbeit mit der/dem TICTS)
- Anpassen und überprüfen der Sicherheitsvorgaben (Allgemeine Richtlinie für Informationssicherheit und Datenschutz, Technische Richtlinie für den Betrieb von Informationssystemen, Weisung Informationssicherheit und Datenschutz, Rollen- und Berechtigungskonzept, Betriebsdokumentation usw.)
- Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
- Berichten an die Schulpflege über den Stand der Informationssicherheit
- Berichten an die Schulpflege über zu treffende Informationssicherheitsmassnahmen und Herbeiführung von Entscheiden
- Erteilung von verbindlichen Anordnungen zur Abwehr von unmittelbar drohenden Gefahren bei Informationssicherheitsvorfällen
- Austausch mit internen und externen Stellen über Informationssicherheitsvorfälle im Bereich Informationssicherheit unter Wahrung der Informationsklassifizierung und Vertraulichkeit, wo nötig
- Beraten der Mitarbeiterinnen und Mitarbeiter, der Schulleitung sowie der Schulpflege in Fragen der Informationssicherheit
- Umsetzung und Pflege des übergreifenden Rollen- und Berechtigungskonzepts (in Zusammenarbeit mit der/dem TICTS)
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
- Bestimmen/Feststellen der Anwendungs- und Datenverantwortlichen

– Sicherstellen, dass alle Mitarbeitenden über die allgemeinen Anforderungen an die Daten- und Informationssicherheit informiert sind und die Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit unterzeichnet haben

5.4 Datenschutzberaterin/Datenschutzberater

Der Datenschutz und die Informationssicherheit sind für alle Bereiche von grundlegender Bedeutung, in denen personenbezogene Daten verarbeitet werden. Die Schulpflege als oberstes Organ trägt die Gesamtverantwortung für den Datenschutz in der Sek Hausen. Die Datenschutzberaterin/der Datenschutzberater arbeitet eng mit der bzw. dem ISV zusammen und ist interne Ansprechperson bei Datenschutzfragen.

Aufgaben der Datenschutzberaterin/des Datenschutzberaters*:
– Ansprechperson für die die ISV, sowie für die Schulleitung und Schulpflege in Belangen des Datenschutzes
– Bindeglied zur kantonalen Datenschutzbeauftragten (DSB) bei Fragen zum Datenschutz
– Zuständige Person für die Einhaltung der gesetzlichen Meldepflicht bei Datenschutzvorfällen
– Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
– Berichten an die Schulpflege über den Stand des Datenschutzes

*Datenschutzberatung durch die WEPAG GmbH, Guido Pellizoni, Rennweg 2, 8932 Mettmenstetten

5.5 Anwendungs- und Datenverantwortliche/Anwendungs- und Datenverantwortlicher

Für alle Prozesse, Daten, Anwendungen, IKT- und Netzwerksysteme werden mehrere verantwortliche Personen benannt.

Aufgaben der/des Anwendungs- und Datenverantwortlichen:
– Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
– Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
– Klassifizieren der Daten, die in ihrem Verantwortungsbereich bearbeitet werden (Vertraulichkeit, Integrität, Verfügbarkeit)
– Verantwortung für den sicheren Betrieb ihrer Anwendung (Vertraulichkeit und Integrität der Datensammlungen, Verfügbarkeit der Anwendung und Datensammlungen)
– Regeln der Massnahmen für die Informationssicherheit sowie deren Kontrolle und Verantwortung
– Kontrollieren der Erfüllung der Datenschutzbestimmungen
– Mitarbeit beim Erstellen von Notfallplänen für längere Ausfälle
– Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensammlungen
– Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Aufbewahrung und Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

5.6 Mitarbeiterinnen und Mitarbeiter

Den Mitarbeiterinnen und Mitarbeitern obliegt eine grosse Verantwortung, da sie durch ihr richtiges Handeln und im Kontakt mit den Betroffenen am meisten für die Sicherstellung des Datenschutzes und der Informationssicherheit beitragen können.

Aufgaben der Mitarbeiterinnen und Mitarbeiter:
– Teilnehmen an Sensibilisierungs- und Schulungsaktivitäten und sicherstellen des Verständnisses
– Einhalten der Gesetze sowie der vertraglichen Regelungen und internen Richtlinien und selbständige Information bei Unsicherheiten

- Unterstützen der Sicherheitsmassnahmen durch eine sicherheitsbewusste Arbeitsweise
- Aufrechterhalten des Risikobewusstseins und Rückfragen bei Unsicherheiten
- Melden von Informationssicherheitsvorfällen und hinweisen auf Schwachstellen an die für die Informationssicherheit verantwortliche Person oder die oder den Vorgesetzten

6 Regelung von Ausnahmen

Die oder der ISV entscheidet über Ausnahmen von den Richtlinien und Weisungen der Sek Hausen. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen und zur Nachvollziehbarkeit zu dokumentieren. Für jede Ausnahme ist ein Zeitpunkt, eine Dauer, die antragsstellende sowie verantwortliche Person zu definieren. Die bestehenden Ausnahmen sind periodisch zu überprüfen.

7 Kontinuierliche Verbesserung der Informationssicherheit

Die Schulpflege unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Sie geben mit der periodischen Überarbeitung dieser Richtlinie zur Informationssicherheit und den dazugehörigen Richtlinien und Weisungen die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung vor. Die Richtlinie wird alle 2 Jahre überprüft.

Die umgesetzten organisatorischen und technischen Massnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit werden regelmässig alle 2 Jahre sowie zusätzlich bei Projekten mit grossen Auswirkungen auf die Aktualität überprüft. Festgestellte Abweichungen sind innert nützlicher Frist zu beheben. Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.

8 Informationssicherheitsmassnahmen

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen. Sie sind angelehnt an die Besonderen Informationssicherheitsrichtlinien des Kantons Zürich.

8.1 Mobiles Arbeiten und mobile Geräte

Der Einsatz von mobilen Geräten inklusive der allfälligen Verwendung von privaten Geräten (Bring Your Own Device) für dienstliche Zwecke durch die Mitarbeiterinnen und Mitarbeiter der Sek Hausen wird in den nächsten zwei Jahren geregelt und dokumentiert.

Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

8.2 Personalsicherheit

Mitarbeiterinnen und Mitarbeiter werden auf die Verpflichtungen in Bezug auf den Datenschutz und die Informationssicherheit hingewiesen:

- Die Verantwortlichkeiten für die Klassifizierung und den Umgang mit Informationen sowie den Umgang mit organisationseigenen Werten
- Die Verantwortlichkeiten im Umgang mit Informationen, die von anderen Organisationen erstellt wurden
- Die Rechte und Pflichten von Mitarbeiterinnen und Mitarbeitern (z.B. Urheberrecht oder Datenschutzgesetz)
- Die Massnahmen, die ergriffen werden, wenn Mitarbeiterinnen oder Mitarbeiter sich nicht an die Bestimmungen halten

Die ISV muss sicherstellen, dass

- alle Mitarbeiterinnen und Mitarbeiter über ihre Verantwortlichkeiten bei klassifizierten Informationen orientiert werden,

- die Richtlinien und Weisungen jederzeit in der neusten Version abrufbar sind,
- das Bewusstsein für Datenschutz und Informationssicherheit geschaffen wird,
- die Fähigkeiten und Qualifikationen von Mitarbeiterinnen und Mitarbeitern durch Schulungen gefördert werden.

8.3 Schulungsmassnahmen in Informationssicherheit

- Alle Mitarbeiterinnen und Mitarbeiter werden regelmässig stufen- und funktionsgerecht auf Informationssicherheitsthemen sensibilisiert und geschult. Neu eintretende Mitarbeiterinnen und Mitarbeiter erhalten zeitnah eine Grundausbildung.
- Schulungen zur Informationssicherheit finden regelmässig statt. Erstausbildung und Schulung gilt für Personen, die in neue Positionen oder Rollen mit wesentlich unterschiedlichen Informationssicherheitsanforderungen wechseln, und nicht nur für Neueinsteiger. Sie finden vor der Aufnahme der neuen Tätigkeit statt.
- Die Sensibilisierungsmassnahmen können eine Reihe von Aktivitäten umfassen wie Kampagnen (z.B. einen «Tag der Informationssicherheit») oder Newsletter.
- Das Bildungs- und Ausbildungsprogramm steht mit den Informationssicherheitsrichtlinien und relevanten Verfahren der Organisation in Einklang und berücksichtigt die zu schützenden Informationen der Organisation sowie die zum Schutz der Informationen durchgeführten Kontrollen. Das Programm berücksichtigt verschiedene Formen der allgemeinen und beruflichen Bildung (z.B. Vorlesungen oder Selbststudien).
- Die Informationssicherheit und das Schutzniveau werden anhand der Aufgabe, Verantwortlichkeit und Empfehlungen vermittelt.
- Die Schulungen werden nachvollziehbar dokumentiert.
- Alle Mitarbeiterinnen und Mitarbeiter, die mobile IKT-Systeme nutzen, werden auf die spezifischen Risiken der Informationssicherheit sensibilisiert (z.B. mit Schulungen). Wenn die Richtlinie für mobile Geräte die Verwendung von mobilen Geräten in Privatbesitz erlaubt, sollten die Richtlinie und die zugehörigen Sicherheitsmassnahmen auch Folgendes berücksichtigen:
  - Trennung der privaten und der geschäftlichen Nutzung der Geräte einschliesslich der Verwendung von Software zur Unterstützung einer solchen Trennung und zum Schutz von Geschäftsdaten auf einem privaten Gerät.
  - Gewährung des Zugangs zu Geschäftsinformationen erst, nachdem die Benutzerinnen und Benutzer die Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit unterschrieben haben, in der die Einhaltung entsprechender Schutzmassnahmen bestätigt wird (physischer Schutz, Software-Aktualisierung etc.).
- Schulungen für Informationssicherheit beinhalten folgende Minimalanforderungen:
  - Das Bekenntnis der Mitarbeiterinnen und Mitarbeiter zur Informationssicherheit der Sek Hausen und angeschlossener Institutionen.
  - Die Notwendigkeit, sich mit der Thematik Informationssicherheit auseinanderzusetzen (z.B. Weisung zur Informationssicherheit).
  - Die persönliche Verantwortung für den Schutz von Informationen.
  - Die Abläufe der Informationssicherheit (z.B. Meldung von Informationssicherheitsvorfällen).
  - Kontaktstellen für zusätzliche Informationen und Beratung zu Fragen der Informationssicherheit und weiterer Schulungsmöglichkeiten.
- Sensibilisierungsmassnahmen zum Thema Datenschutz.

Neue Mitarbeiterinnen und Mitarbeiter unterzeichnen bei Stellenantritt die Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit.

8.4 Verschlüsselungsmassnahmen

Bei Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen wie besondere Personendaten, erfolgt die Speicherung und Übermittlung verschlüsselt. Zur Anwendung kommen aktuelle Verschlüsselungsverfahren.

8.5 Verwaltung von organisationseigenen Werten

Sämtliche für den Betrieb notwendigen organisationseigenen Werte werden in einem aktuellen Inventar geführt (Informationen, Anwendungen, Systeme usw.). Die Verantwortlichkeiten werden ebenfalls im Inventar erfasst.

Die IKT-Umgebung ist dokumentiert (z.B. in Form einer Betriebsdokumentation).

8.6 Informationshandhabung

Informationen werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen. Die Vertraulichkeit ist jederzeit sicherzustellen. Musterbriefe für Auskunft, Informationszugang und Datensperre stehen auf der Website der DSB des Kantons Zürich www.datenschutz.ch zur Verfügung.

Die Sek Hausen bewertet bei einer beabsichtigten neuen Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen (Datenschutz-Folgenabschätzung). Sie unterbreitet eine solche vorab der DSB zur Prüfung (Vorabkontrolle), wenn die Bearbeitung von Personendaten besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhält (§10 IDG).

Informationen werden nach Ablauf der vorab definierten Aufbewahrungsdauer dem zuständigen Archiv angeboten. Informationen, die das zuständige Archiv nicht übernimmt, werden sicher vernichtet.

8.7 Verwendung von Wechselmedien

Der Einsatz von Wechselmedien erfolgt kontrolliert, darauf enthaltene dienstliche Daten werden vor Zugriff von Dritten und Verlust geschützt.

8.8 Identitäts- und Zugriffskontrolle

Organisationseigene Werte werden mit geeigneten Massnahmen vor nicht autorisiertem Zugang und Zugriff geschützt. Dieser Schutz umfasst die Authentifizierung (Prüfung, ob die Nutzerin/der Nutzer derjenige ist, für den sie/er sich ausgibt) und Autorisierung (Prüfung, ob die Nutzerin/der Nutzer zugriffsberechtigt ist).

Es gelten die folgenden Grundsätze:

- Der Zugriff auf die Informationen ist durch ein Rollen- und Berechtigungskonzept geregelt (siehe auch Vorlage Rollen- und Berechtigungskonzept).
- Berechtigungen werden nach einheitlichen Prozessen vergeben, angepasst und auch wieder gelöscht (siehe auch Vorlage Rollen- und Berechtigungskonzept).
- Die Zugriffsberechtigungen für Behördenmitglieder, Mitarbeiterinnen und Mitarbeiter sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.
- Technische Konten und Benutzerkonten sind einer verantwortlichen Person zugewiesen.
- Zugriffsrechte für Mitarbeiterinnen und Mitarbeiter werden mindestens jährlich geprüft. Administrative Zugriffsrechte werden mindestens halbjährlich geprüft.
- Bei Abteilungs- oder Aufgabenwechsel von Mitarbeiterinnen und Mitarbeitern werden die Zugriffsrechte geprüft und wenn nötig angepasst.
- Bei Austritt von Mitarbeiterinnen und Mitarbeitern werden deren Zugriffsrechte umgehend entfernt bzw. deaktiviert. Verwaltungseigene Hardware wird spätestens bei Austritt zurückgenommen.

- Die Art und Stärke der Authentifizierung werden durch die Klassifizierung der Information und die Exponiertheit der Anwendung bestimmt, auf die der Zugriff erfolgen soll.
- Zugriffsrechte für administrative Zugriffe werden restriktiv und kontrolliert vergeben.
- Es ist jederzeit nachvollziehbar, wer welche Zugriffsrechte besitzt.

Bei der Berechtigungsvergabe gelten die allgemeinen Grundsätze:
- Need-to-know: Der Zugriff ist nur auf die Informationen gestattet, die zur Durchführung der Aufgabe benötigt werden.
- Least-privilege: Es sind nur die Berechtigungen zuzuweisen, die zur Durchführung der Aufgabe benötigt werden.
- Segregation of Duties: Zur Vermeidung von Interessenkonflikten ist die Funktionstrennung zu gewährleisten.

8.9 Passwörter

Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch persönliche Passwörter gesichert. Es wird eine ausreichende Qualität und Schutz der Passwörter sichergestellt.

8.10 Physische Sicherheit und Schutz vor Umwelteinflüssen

Zutritt

Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem geschützt. Die Zutrittsberechtigungen werden verwaltet und restriktiv vergeben.

Physische Sicherheit

Gebäude und Räume sowie IKT- und Netzwerksysteme werden mit angemessenen Massnahmen gegen Umwelteinflüsse wie Feuer, Wasser, Feuchtigkeit, Rauch, gegen Einbruch und Diebstahl sowie Stromausfall geschützt. Es sind entsprechende Alarmierungs- und Meldeanlagen vorhanden.

8.11 Sicherheit von Informationssystemen

Neue Informationssysteme werden im Inventar der Sek Hausen nachgeführt, bei Bedarf werden die Auswirkungs- und Bedrohungsanalyse und die Schutzmassnahmen angepasst.

Neue Informationssysteme werden vor ihrer Inbetriebnahme auf ihre Kompatibilität mit bestehenden Systemen geprüft, getestet und abgenommen. Vor der produktiven Inbetriebnahme liegt eine Dokumentation der Systeme vor.

Alle Informationssysteme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.

Bei der Evaluation und Beschaffung von Anwendungen werden deren Sicherheitsfunktionen berücksichtigt.

Die Informationssysteme werden nach der Beschaffung sicher installiert, konfiguriert und betrieben (gemäss anerkannten Sicherheitsstandards), mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.

Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft. Sicherheitsrelevante Ereignisse werden aufgezeichnet und periodisch oder bei Verdacht ausgewertet.

Schwachstellen für Informationssysteme und Anwendungen werden laufend überprüft und gemäss ihrer Kritikalität behandelt (z.B. durch Updates oder Austausch).

Informationen zu Verwaltungstätigkeiten werden bei der elektronischen Übertragung und dem physischen Transport in Abhängigkeit ihrer Schutzstufe vor unbefugter Kenntnisnahme und Bearbeitung geschützt.

Beim Austausch von elektronischen oder physischen Informationen mit externen Organisationen und Personen werden die folgenden Anforderungen in Abhängigkeit von der Klassifizierung der auszutauschenden Informationen geprüft und, falls erforderlich, vertraglich geregelt:
- Verfahren zur Sicherstellung der Nachvollziehbarkeit.
- Einsatz von kryptografischen Verfahren gemäss Kapitel 8.4.
- Aufrechterhaltung einer Informationskette (z.B. Sendungsverfolgung, Empfangsbestätigung) während der elektronischen Übertragung.
- Definierte Zugangskontrollen und Verfahren, die Informationen und physische Datenträger während des physischen Transports schützen.

Falls für die Telefonie internetbasierte Systeme eingesetzt werden, so ist gewährleistet, dass diese den damit verbundenen Risiken entsprechend sicher eingerichtet und betrieben werden (z.B. Netztrennung, angemessene Zugriffsrechte, Ausfallsicherheit, Sicherheitskonfiguration, vertragliche Absicherungen).

Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
Die Ausserbetriebnahme und die fachgerechte Entsorgung von Informationssystemen erfolgen nach einem dokumentierten Prozess. Bei der Ausserbetriebnahme oder einer Reparatur von Informationssystemen müssen Informationen irreversibel gelöscht werden, bevor die Informationssysteme ausgetauscht, entsorgt oder wiederverwendet werden. Dies gilt besonders bei IKT-Systemen mit Speichermedien (z.B. mobile Endgeräte, Drucker, Kameras).

8.12 Datensicherung und -wiederherstellung

Datensicherungen werden regelmässig durchgeführt. Es ist sichergestellt, dass Datensicherungen geographisch abgetrennt von den produktiven Daten aufbewahrt und vor Zugriff geschützt werden.

Die Datensicherungen werden entsprechend den rechtlichen Anforderungen aufbewahrt (siehe Kapitel 8.20 Aufbewahrung und Archivierung).

Es ist gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.

8.13 Protokollierung

Aktivitäten der Benutzerinnen und Benutzer auf den IKT-Systemen der Sek Hausen können aus Gründen der Nachvollziehbarkeitspflicht wie auch der Funktionsüberwachung, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet werden.

Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin respektive des Benutzers möglich.

8.14 Verwaltung der Netzwerksicherheit

Das Netzwerk wird in Sicherheitszonen unterteilt und alle Netzwerkzugänge werden mit Firewalls gesichert. Wo ausschliesslich eine Leunet-Verbindung verwendet wird, kann auf eine zusätzliche Firewall verzichtet werden. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern.

Die Installation und der Betrieb von Netzwerkkomponenten erfolgen gemäss den Sicherheitsvorgaben der Technischen Richtlinie für den Betrieb von Informationssystemen (siehe entsprechende Vorlage). Bei Verwendung von WLAN-Netzen wird auf eine Abtrennung der Netze sowie auf Zugriffsrechte und Verschlüsselung geachtet.

Die Vorgaben des Kantons Zürich in Bezug auf den Anschluss an das übergeordnete Netzwerk (Leunet) werden eingehalten.

8.15 Sicherheit von Testdaten

Für Testsysteme sind die gleichen Sicherheitsanforderungen umzusetzen, wie dies bei Produktivsystemen der Fall ist. Diese Anforderung gilt besonders dann, wenn auf Testsystemen mit Testdaten aus produktiven Systemen (Datenkopien) gearbeitet werden muss. In diesen Fällen ist die Anzahl der verwendeten vertraulichen Daten auf ein Minimum zu beschränken. Nach durchgeführten Tests sind die Informationen zu löschen. Über die Verwendung von Tests mit Daten aus produktiven Systemen ist ein Protokoll zu führen. Wenn immer möglich sind Tests mit anonymisierten oder pseudonymisierten Daten durchzuführen.

8.16 Auslagerung von Datenbearbeitungen (Outsourcing)

Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.
Jeder Outsourcing-Vertrag enthält mindestens Regelungen zu folgenden Themen:

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (immer beim öffentlichen Organ)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen (Voraussetzungen für Bekanntgabe an Dritte)
- Geheimhaltungsverpflichtungen (Hinweis auf Amtsgeheimnis)
- Rechte Betroffener (Umgang mit Auskunftsbegehren)
- Informationssicherheitsmassnahmen (organisatorisch/technisch)
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung)
- Entwicklung und Wartung (Regelung für den Beizug Dritter)
- Orte der Datenbearbeitung (Schweiz, Ausland mit gleichwertigem Datenschutzniveau, ansonsten Schutz durch zusätzliche Massnahmen)
- Cloud Computing (wenn genutzt, den zusätzlichen Risiken angepasste Massnahmen)
- Sanktionen (Konventionalstrafe für schwere Vertragsverletzungen)
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Verhältnis zu allgemeinen Vertragsbedingungen (wenn vorhanden, Vorrang des Vertrags)
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand im Kanton Zürich)

Für ausgelagerte Leistungen und Produkte werden Dienstgütevereinbarungen (Service Level Agreements) abgeschlossen. Sie definieren und quantifizieren:

- Inbegriffene Leistungen und Produkte
- Mengengerüste, Kapazität, Anzahl Transaktionen etc.
- Betriebszeiten
- Maximale Ausfalldauer pro Vorfall (Recovery Time Objective, RTO)
- Maximaler Datenverlust bei einem Ausfall (Recovery Point Objective, RPO)
- Supportzeiten
- Reaktions- und Umsetzungszeiten

- Lösungszeiten
- Kommunikationspartner und Eskalationspfad
- Im Preis inbegriffene Leistungen, Verrechnungseinheiten, Preise für weitere Leistungen
- Kontrollmittel zur Überwachung der Leistungen
- Notfallszenarien und -massnahmen

Falls Cloud-Lösungen (nicht zu verwechseln mit klassischen Auslagerungslösungen) in Anspruch genommen werden sollen, so ist nach dem Merkblatt Cloud Computing sowie dem Leitfaden Auslagerung: Berücksichtigung des CLOUD Act der DSB des Kantons Zürich vorzugehen, zudem sind die obengenannten Anforderungen einzuhalten.

Benötigt eine externe Stelle oder der interne IKT-Betrieb den Einsatz von Fernwartungszugängen, werden diese nur nach entsprechendem Antrag freigegeben und auf die nötigsten Systeme und Zeiten begrenzt.
Vor der Gewährung von Fernwartungszugängen erfolgt eine angemessene Sicherheitsüberprüfung, eine Geheimhaltungsverpflichtung wird unterzeichnet und entsprechende vertragliche Regelungen werden abgeschlossen. Dasselbe gilt für den Einsatz von Fremdpersonal (z.B. temporäre Mitarbeiterinnen oder Mitarbeiter).

8.17 Umgang mit Informationssicherheitsvorfällen

Bei Informationssicherheitsvorfällen erfolgt durch die bzw. den ISV eine Klassifizierung und wenn nötig sofortige Rapportierung an die Schulpflege. Entsprechende interne Prozesse und Verfahren für Meldung, Aufnahme von Beweismitteln zwecks rechtlicher und/oder disziplinarischer Massnahmen sowie eine angemessene Eskalation sind geregelt (siehe dazu auch Notfallkonzept).

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):
- Verlust, unberechtigte bzw. unbeabsichtigte Löschung oder Vernichtung von Daten, Kopien von Daten oder von Datenträgern
- Veränderung oder Manipulation von Informationen
- Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
- Funktionalität eines oder mehrerer Informationssysteme gestört oder nicht mehr vorhanden

Bei meldepflichtigen Informationssicherheitsvorfällen (Gefährdung von Grundrechten durch die unbefugte Bearbeitung oder den Verlust von Personendaten) erstattet die Schulpflege unverzüglich nach Bekanntwerden des Vorfalls bei der DSB Meldung (§ 12a IDG). Bei Zweifeln über das Vorliegen einer Meldepflicht erfolgt eine unverzügliche Kontaktaufnahme mit der DSB. Im Notfallkonzept sind mögliche Informationssicherheitsvorfälle und Massnahmen zu definieren.

Alle Informationssicherheitsvorfälle werden nachvollziehbar dokumentiert. Die Informationen sind als vertraulich zu betrachten.

8.18 Drucker, Kopierer und Multifunktionsgeräte

Drucker, Kopierer und Multifunktionsgeräte können eine Vielzahl von vertraulichen Daten speichern. Standort und Berechtigungen auf solchen Geräten werden daher entsprechend sorgfältig gewählt, so dass keine Daten durch Dritte eingesehen werden können.

Es ist sichergestellt, dass die Geräte einen möglichst hohen Sicherheitsstandard aufweisen bzw. so sicher wie möglich konfiguriert werden.

Mit den Lieferanten der Geräte werden Wartungsverträge und Datenschutzbestimmungen vereinbart.

Wenn Geräte die Räumlichkeiten der Sek Hausen verlassen, wird sichergestellt, dass sich darauf keine Daten mehr befinden.

8.19 Aufbewahrung und Archivierung

Informationen, die für das Verwaltungshandeln nicht mehr benötigt werden, werden während höchstens zehn Jahren weiter aufbewahrt. Eine längere Aufbewahrungsdauer wird nur in Fällen angewendet, in denen abweichende gesetzliche Fristen zur Anwendung kommen. Die Begründung für die Wahl einer längeren Aufbewahrungsfrist wird dokumentiert.

Nach Ablauf der Aufbewahrungsfrist werden die Informationen dem zuständigen Archiv angeboten. Allen mit der Aufbewahrung von Informationen betrauten Mitarbeiterinnen und Mitarbeiter ist bekannt, an welches Archiv die Informationen anzubieten sind.
Informationen, die vom zuständigen Archiv nicht übernommen werden, sind endgültig zu löschen bzw. ordnungsgemäss zu vernichten.

8.20 Risikoanalyse / Notfallplanung

Für die Sek Hausen wird eine Auswirkungs- und Bedrohungsanalyse geführt (siehe entsprechende Vorlage). Es werden gemäss der Risikoabschätzung geeignete Massnahmen definiert und umgesetzt.

Die Risikoanalyse dient ebenfalls als Grundlage für das Notfallkonzept der Sekundarschule Hausen am Albis (siehe entsprechende Vorlage). Das Notfallkonzept beschreibt die Notfallplanung für Geschäftsprozesse und/oder Ressourcen (Schutzobjekte), um die Aufrechterhaltung und Wiederherstellung der ordnungsmässigen Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.

Die Notfallmassnahmen sind regelmässig und bei veränderten Rahmenbedingungen zu überprüfen und zudem regelmässig zu testen.

Details sind im Notfallkonzept und der Auswirkungs- und Bedrohungsanalyse zu finden.

9 Genehmigung und Inkrafttreten

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und/oder personalrechtliche Konsequenzen haben.

Die Schulpflege beauftragt die ISV, alle für die Umsetzung dieser Richtlinie benötigten Dokumente in Zusammenarbeit mit den betroffenen Stellen bis Mai 2027 auszuarbeiten.

Beschlossen durch die Schulpflege mit Beschluss [Nr.] am [Datum].

Esther Flückiger
Schulpräsidentin

Barbara Moser
Ressort Informatik und Kommunikation

Anhang A – Organigramm Sekundarschule Hausen am Albis

Die Informationssicherheitsorganisation der Sek Hausen gemäss Organigramm vom August 2025: